シャンノンの通信路符号化定理周辺の未解決問題

様式 C-19

科学研究費補助金研究成果報告書

平成 23 年 6 月 1 日現在

機関番号：32675
研究種目：基盤研究（C）
研究期間：2008～2010
課題番号：20560372
研究課題名　シャンノンの通信路符号化定理周辺の未解決問題
研究課題名　Shannon’s channel coding problems from points of view of both information theory and algebraic coding theory
研究代表者
西島　利尚（NISHIJIMA TOSHIHISA）
法政大学・情報科学部・教授
研究者番号：70211456

研究成果の概要(和文):シャノンの通信路符号化定理の周辺に存在する未解決問題に関連して，2 元線形ブロック符号全体の集合族の能力を評価する指標として，信頼度関数・漸近的距離比・見逃し誤り確率のそれぞれに対して限界式が与えられている．従来の研究では，信頼度関数と漸近的距離比との関係は明らかにされていないが，見逃し誤り確率と漸近的距離比，見逃し誤り確率と信頼度関数のそれぞれについては重要な関係が明らかにされている．そこで特徴的な構造を持つ 2 元線形ブロック符号の重要な部分クラスの集合族に対して，信頼度関数・漸近的距離比・見逃し誤り確率のそれぞれの限界式を与え，2 元線形ブロック符号のそれらと比較しつつ，それぞれの関係を明らかにしていくことは重要な研究分野である．本研究成果は，(1) シャノンの通信路符号化定理を具体的に満足する漸近的に能率の良い符号である Justesen 符号の低符号化比率における収束点を明らかにした．(2) 2 値展開された一般化リードソロモン符号の見逃し誤り確率の正確な値は，その符号の 2 元重み分布が陽に与えられなければ計算できない．そこで，最大距離分離符号が有するハミング重み分布の特徴的な構造，すなわち，符号語を情報記号部と検査記号部とに分離し，それぞれの部分のハミング重み分布を陽に求め，その分布を用いて見逃し誤り確率の上界および下界を計算するための 2 元重み母関数を与えた．(3) $GF(2^m)$で構成される Wozencraft のランダムシフト符号とその集合族が有する 2 元重み分布多項式について、一般的かつ基本的な性質のいくつかを明らかにした．

研究成果の概要(英文):It is well known that each bound of reliability function, asymptotic distance ratio, and the probability of undetected error for the ensemble of all binary linear block codes is given. Therefore we think that it is an important research to get each bound of those functions for an ensemble of some important subclasses of binary linear block codes in order to find a clue to a solution for some open problems in information theory or the theory of error correcting codes. (1) By using a feature structure of the Justesen code, the convergent points of the asymptotic distance ratio that those families have are specified on the basis of not a lower bound but minimum weights obtained from those weight distributions. (2) By utilizing certain characteristic structure of the Hamming weight distribution of maximum distance separable codes, we can get weight enumerators to compute an upper and a lower bound on the probability of an undetected error for binary expansions of generalized Reed-Solomon codes. Also, values of the average probability of an undetected error are computed by using the average weight distribution for an ensemble of binary expansions of all codewords of all Reed-Solomon codes for some given concrete code parameters. (3) We show some properties of the weight enumerators of all the codes over $GF(2^m)$ in Wozencraft’s ensembles of randomly shifted codes

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	800,000	240,000	1,040,000
2009 年度	700,000	210,000	910,000
2010 年度	700,000	210,000	910,000
総　計	2,200,000	660,000	2,860,000

研究分野：工学
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：情報理論、符号理論

１．研究開始当初の背景

シャノンの通信路符号化定理は，「通信路容量 C を超えない正の値の情報伝送速度 R で，符号長 N とするとき，復号誤り確率 $P(\varepsilon)$ が，$P(\varepsilon) \leqq \exp\{-NE(R)\}$ で与えられる．」ことを主張している．ここで，$E(R)>0$ が信頼度関数と呼ばれている．そしてこの結論を具体的に満足する誤り訂正符号を構成するための理論体系が符号理論である．情報理論とは独立に体系づけられる符号理論において，誤り訂正符号の信頼性の評価は，漸近的距離比 $\delta(R)$ により行われる．漸近的距離比 $\delta(R)$ は，誤り訂正符号の符号長 N を大とするとともに訂正可能な誤りの個数を符号長 N との比で表したものである．

シャノンの通信路符号化定理は，A. Feinstein, R. M. Fano, R. G. Gallager, A. J. Viterbi, 有本卓, I. Csiszar, J. Korner, R. E. Blahut そして韓太舜らにより現代化，精密化，定量化，そして一般化されてきている．特に，1970 年代後半から I. Csiszar, J. Korner と R. E. Blahut 等により“タイプの概念”を用いて，通信路の特性に依存しない符号化・復号化によるユニバーサルな通信路符号化定理が導出された．これによって，通信路符号化に対する新しい視点や解釈が与えられ，定理の一般化がなされてきた．また，韓太舜は“情報スペクトルの概念”を用いて，自然な一般化を行い，情報理論の再構築を試みている．しかし，信頼度関数 $E(R)$ は，低情報伝送速度 R では信頼度関数 $E(R)$ の上界と下界との間には差があり真の値は未だに求められていない．

一方，符号理論の立場から，復号誤り確率 $P(\varepsilon)$ の下界は漸近的距離比 $\delta(R)$ の上界が与え，復号誤り確率 $P(\varepsilon)$ の上界は漸近的距離比 $\delta(R)$ の下界が与えるから，2 元対称通信路においては漸近的距離比 $\delta(R)$ を正確に求めることが信頼度関数 $E(R)$ を正確に求めることに対応する．現在のところ，その漸近的距離比 $\delta(R)$ の最も強い上界は，R. J. McEliese, E. R. Rodimich, H. Rumsey, Jr. と L. R. Welch によって与えられており，下界は Varshamov-Gilbert の下界式が最も強い限界式である．両者の間にはまだ隔たりがある．この隔たりを埋めることは，「漸近的距離比 $\delta(R)$ が Varshamov-Gilbert の下界式を等式で満足するならば，削除誤り指数 $E_{ex}(R)$ が真の信頼度関数 $E(R)$ を与える」という Shannon 等による仮説に対応している．これは未だに仮説であり証明されていない．

さらに，J. Justesen は，連接符号化によって Varshamov-Gilbert の下界式には到底及ばないまでも，漸近的距離比 $\delta(R)$ が正である漸近的に能率の良い符号をはじめて構成的に与え，シャノンの通信路符号化定理を非ランダムな符号化による証明を試みた．その後，主として杉山康夫等によって，Justesen 符号の大幅な改良がなされている．

また，符号理論の中には，任意に与えられた 2 元線形符号の重み分布を解析的に求める問題と非 2 元線形符号，すなわちリードソロモン符号等のガロア体のシンボル単位での重み分布（完全重み分布）を陽に求める問題が未解決問題として残されている． 前者の問題は，嵩忠雄による BCH 符号や Reed-Muller 符号の研究成果が大半を占め，後者の問題にいたっては，I. F. Blake と常盤欣一朗のリードソロモン符号の情報記号数の極めて小さな値での研究成果があるのみである．任意の符号の重み分布を陽に与えることは，その与えられた符号の復号誤り確率 $P(\varepsilon)$，見逃し誤り確率 $P_u(\varepsilon)$ や漸近的距離比 $\delta(R)$ を直接，正確に与えることを意味しており，シャノンの通信路符号化定理を非ランダムな構成的符号化による証明を与えることと等価である．

以上本研究課題は，主として Shannon の A Mathematical Theory of Communication が発表されて以来の古典的ではあるが，情報科学の研究領域において，その解決は極めて本質的なの未解決問題である．

２．研究の目的

本研究は，シャノンの通信路符号化定理の証明に関わる未解決問題に情報理論的立場及び符号理論的立場の両側面からアプローチし，両側面の相互の関係を明らかにしつつ，最終的に下記の 3 つの未解決問題の解決を主たる目的とした．

(1) 低情報伝送速度 R での信頼度関数 $E(R)$ の真の値を求める．あるいは，Shannon 等による仮説の証明を与える．
(2) ランダム符号化により証明された通信路符号化定理を非ランダムな構成的符号化により証明する．
(3) 任意に与えられた 2 元線形符号の重み分布と任意に与えられた非 2 元線形符号の完全重み分布を解析的に求める．

３．研究の方法

(1)の問題に対しては，小林欣吾，韓太舜，“再考：誤り指数あれこれ”，情報理論とその応用学会ワークショップ講演資料，pp. 104-120,

1993年，が最も重要な論文と考えている．上述の3つのテーマの中で，最も基礎的な問題であるから，文献調査が中心となるのは必須である.この論文を中心として1993年以前，以後の鍵となる論文の検討から研究をスタートし，派生する問題，解決の糸口となりうる問題を発見し，その解析を行っていく．
(2)の問題に対しては，Justesen 符号は，原始リードソロモン符号とそれにある種の一般化を施すことによって得られる一般化リードソロモン符号との連接によって得られる符号である．これら2種類のリードソロモン符号の連接こそが，全体としての2元最小重みの増加を図っていると解釈できる．この解釈を手がかりとして，原始リードソロモン符号を基に，それにいかなる一般化を施せば，得られた一般化リードソロモン符号を2値に展開した際の最小重みが，元の原始リードソロモン符号を2値展開した符号の最小重みを確実に上回ることができるかを探って行く．同時に，漸近的に能率の良い符号の改良のために，これらの手法を一般化連接符号に適用できないかを解析する．
(3)の問題に対しては，直接 2 元重み分布あるいは完全重み分布を解析的に求めることは極めて困難ゆえ，2 元線形ブロック符号の重要な部分クラスの符号の集合族に対して，平均見逃し誤り確率の上界を求めそれぞれ比較して行く．特に，シャノンの通信路符号化定理を満足する重要部分クラスである連接符号・繰り返し符号の集合族に対して比較検討をする．

以上述べたとおり本研究課題は，1948年に情報理論が発足して以来の情報理論の中の主たる未解決問題の解決を目的としているので，極めて独創的，基礎的であることは言うまでもない．しかし，極めて独創的，基礎的であるがゆえに研究成果が簡単には出ない．したがって，本質的な問題の解決には至らないまでも上述した3つの未解決問題から派生するいくつかの問題，あるいは解決の糸口となりうるいくつかの問題の解析を地道に行っていくことが極めて重要な研究となる．具体的には，各年度において下記の研究会，ワークショップ，シンポジウムに参加・発表することによって本研究を遂行した．そして，口頭発表した研究内容は，可能な限り論文としてまとめ，電子情報通信学会基礎境界ソサエティの論文誌への投稿を試みた．

【国内】
(1)情報理論とその応用シンポジウム(SITA)
(2)シャノン理論ワークショップ（STW）
(3)電子情報通信学会情報理論専門委員会研究会（情報理論研究会）

【国外】
(1) International Symposium on Information Theory (ISIT)
(2) Asian-European Workshop on Information Theory (AEW)
(3) International Symposium on Information Theory and Its Applications (ISITA)

４．研究成果

具体的な成果は，研究期間内に電子情報通信学会論文誌に公開した3件の論文の概要により示す.
(1)「低符号化比率の Justesen 符号に対する漸近的距離比の収束点」

E. Kolev や鴻巣と常盤は，極めて限られたパラメータではあるが，Justesen 符号の特徴的な構造を用いて，いくつかの集合族に対してそれらの2元重み分布を陽に与えた．しかし，これらの集合族に対する漸近的な評価は与えられていない．そこで本論文では，これらの 2 元重み分布が陽に与えられている Justesen 符号のいくつかの集合族に対して，下界式による評価ではなく，それらの集合族が有する漸近的距離比の収束点を特定した．そして，2 元重み分布が陽に与えられている Justesen 符号の集合族が有する漸近的な能力の位置付けを明確に示した．
(2)「2 値に展開された連接符号の見逃し誤り確率の上界と下界について」

2 値展開された一般化リードソロモン符号の見逃し誤り確率に着目した．2 値展開された一般化リードソロモン符号の見逃し誤り確率の正確な値は，その符号の2元重み分布が陽に与えられなければ計算できない．そこで，最大距離分離符号が有するハミング重み分布の特徴的な構造，すなわち，符号語を情報記号部と検査記号部とに分離し，それぞれの部分のハミング重み分布を陽に求め，その分布を用いて見逃し誤り確率の上界および下界を計算するための2元重み母関数を与えた．そして，具体的な符号パラメータに対して，これらの母関数を用いて見逃し誤り確率の上界および下界の数値例を示した．さらに，2 値展開された一般化リードソロモン符号の全てを含む集合族上に与えられる平均重み分布を用いて，その集合族上の平均見逃し誤り確率を計算し，そして上界および下界の数値例と比較し，本論文で提案する2元重み母関数が見逃し誤り確率の上界および下界を計算する上で極めて有効であることを示した．
(3)「Wozencraft のランダムシフト符号とその集合族が有する2元重み分布多項式に関するいくつかの性質」

Justesen 符号の内部符号として用いられ，その集合族に Varshamov-Gilbert の下界式を満たす符号が存在する $GF(2^m)$ で構成される Wozencraft のランダムシフト符号とその集合族が有する 2 元重み分布多項式について，

一般的かつ基本的な性質のいくつかを明らかにした.
(4)「積符号と連接符号の集合族上に与えられる平均見逃し誤り確率の上界式の比較」
組織的な2元線形ブロック符号の集合族上に与えられる平均見逃し誤り確率の上界式を導出した手法を積符号および連接符号の集合族上に直接適用し，それぞれの集合族上に与えられる平均見逃し誤り確率の上界式を陽に求める．そして，求めたそれぞれの上界式を直接比較することにより集合族がもつ平均的な能力を比較する．その結果，積符号より連接符号の方が優れていることを明らかにする．同時に，連接符号の平均的な能力は2元線形ブロック符号のそれには及ばないことも明らかにする.
これは学会発表⑦の Upper bounds on the average probability of an undetected error for the ensemble of both product and concatenated codes の内容を電子情報通信学会論文誌へ投稿中である.
(5)「積符号と連接符号の漸近的距離比の下界式の比較」
学会発表済みの内容を電子情報通信学会論文誌へ投稿準備中である.
(6)「可変内部符号化された 2 元連接符号の集合族上に与えられる平均見逃し誤り確率の上界式について」
学会発表済みの内容を電子情報通信学会論文誌へ投稿準備中である.

５．主な発表論文等
〔雑誌論文〕（計3件）

① 鴻巣敏之、西島利尚、常盤欣一朗、低符号化比率の Justesen 符号に対する漸近的距離比の収束点、電子情報通信学会論文誌、査読あり、Vol. J91A No.5、2008、pp. 587-590
② 西島利尚、2 値に展開された連接符号の見逃し誤り確率の上界と下界について、電子情報通信学会論文誌、査読あり、Vol. J92A No.1、2009、pp. 48-54
③ 鴻巣敏之、西島利尚、常盤欣一朗、Wozencraft のランダムシフト符号とその集合族が有する 2 元重み分布多項式に関するいくつかの性質、電子情報通信学会論文誌、査読あり、Vol. J92A No.4、2009、pp. 724-726

〔学会発表〕（計7件）

① 西島利尚、常盤欣一朗、鴻巣敏之、Wozencraft のランダムシフト符号とその集合族が有する 2 元重み分布多項式に関するいくつかの性質、電子情報通信学会技術研究報告、IT-2008-35、2008.9.12、pp.91-94、カルチャーリゾート・フェストーネ（沖縄県宜野湾市）
② 遠藤寿之、西島利尚、常盤欣一朗、鴻巣敏之、原始リード - ソロモン符号の 2 元重み分布のクラス分けについて、電子情報通信学会技術研究報告、IT-2008-36、2008.9.12、pp.95-98、カルチャーリゾート・フェストーネ（沖縄県宜野湾市）
③ 西島利尚、常盤欣一朗、鴻巣敏之、一般化リード - ソロモン符号の集合族における原始リード - ソロモン符号の特定、第31回情報理論とその応用シンポジウム予稿集、2008.10.9、pp. 724-726、鬼怒川温泉あさやホテル
④ 西島利尚、常盤欣一朗、積符号の信頼度関数・漸近的距離比・見逃し誤り確率について、電子情報通信学会技術研究報告、IT-2008-112、2009.3.10、pp.453-457、公立はこだて未来大学
⑤ 西島利尚、常盤欣一朗、連接符号の信頼度関数・漸近的距離比・見逃し誤り確率について、電子情報通信学会技術研究報告、IT-2009-31、2009.7.24、pp.147-152、関西学院大学
⑥ 西島利尚、常盤欣一朗、可変内部符号化された 2 元連接符号の集合族上に与えられる平均見逃し誤り確率の上界式について、電子情報通信学会技術研究報告、IT-2008-112、2009.9.25、pp.453-457、愛媛大学
⑦ T. Nishijima and K. Tokiwa, Upper bounds on the average probability of an undetected error for the ensemble of both product and concatenated codes, The 2010 International Symposium on

Information Theory and Its Applications, 査読あり, 2010.10.17-20、台湾（台中市）

６．研究組織
(1)研究代表者
西島　利尚（NISHIJIMA　TOSHIHISA）
法政大学・情報科学部・教授
研究者番号：70211456